

Artículo

Pagos, micropagos e internet

Por Cristina García Testal

Resumen: Introducción al panorama del comercio electrónico: aspectos de seguridad, legales, técnicos... Se analizan distintos proyectos ya en marcha, así como se hace una prospección de lo que estas aplicaciones podrían suponer en el ámbito de las bibliotecas y los centros de documentación.

Palabras clave: Comercio electrónico, Micropagos, Bibliotecas, Centros de documentación.

Title: Payments, micropayments and internet

Abstract: A general introduction to electronic commerce is provided, covering security, law and technology. Several projects already operational in this area are analysed as well as the implications they might have for the library world.

Keywords: Electronic Commerce, Micropayments, Libraries.

García Testal, Cristina. "Pagos, micropagos e internet". En: *El profesional de la información*, 2000, marzo, v. 9, n. 3, pp 11-19.



Cristina García Testal

EL COMERCIO ELECTRÓNICO se puede definir como cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación como internet¹. Esto lleva a enfrentarse a la pregunta de dónde reside el valor del dinero, qué es lo que hace que se acepte comúnmente como algo valioso. Son preguntas de la era digital, iguales a las que surgieron con la aparición de las primeras monedas, cuando se abandonó la idea de fabricarlas con metales preciosos, es decir: cuando dejaron de tener valor en sí mismas. Las preguntas idénticas que se formularon frente a los primeros billetes en papel, con los cheques o con las tarjetas de crédito.

En muchos sentidos, internet es el gran escaparate al que se asoman a diario millones de consumidores, un mercado de rápido crecimiento donde los canales de distribución son baratos, cómodos y rápidos. Las empresas han encontrado así una nueva manera de publicitar su mercancía, para venderla de forma directa eliminando intermediarios y canales de distribución, para establecer nuevas formas de cooperación entre compañías, un medio para ampliar mercados accediendo a nuevos consumidores y para mejorar también sus servicios de atención al cliente.

Desde el punto de vista del consumidor, internet es también un nuevo mercado que abre la posibilidad de acceder a casi cualquier producto y comparar ofertas y le permite intercambiar información sobre un servicio determinado. Este grupo es especialmente sensible a la reducción de precios, la rapidez en la entrega y los servicios de valor añadido.

También el comercio electrónico plantea nuevas cuestiones que hay que solucionar: la validez legal de las transacciones, la necesidad de una armonización

internacional que haga las distintas legislaciones nacionales compatibles, que el sistema de dinero electrónico que favorece la absoluta privacidad no sea un pozo de blanqueo de dinero, la protección del consumidor frente a la publicidad engañosa, la utilización fraudulenta de datos personales o la seguridad de los medios de pago electrónicos.

Estos problemas se mezclan con las dificultades locales propias de la situación particular de cada país y de lo avanzadas que se encuentren las telecomunicaciones. No es lo mismo implantar un nuevo sistema en EUA que iniciar su incursión en países como España, Portugal o Italia.

En España actúan como factores negativos la falta de cultura empresarial en la utilización de la Red, los hábitos de los consumidores —tanto en el aspecto lúdico de la compra como en la falta de familiaridad con la informática— la baja penetración del ordenador y de internet, desconocimiento del medio, falta de información sobre los sistemas de pago y desconfianza en su seguridad, lo que está retrasando la evolución del comercio electrónico.

«Internet es un mercado de rápido crecimiento donde los canales de distribución son baratos, cómodos y rápidos»

Para el usuario uno de los factores negativos resaltados más reiteradamente es la lentitud de carga de las páginas web o los enlaces que apuntan a otras que ya no existen. Otro problema que les afecta es la diversidad de procedimientos de compra, de tal forma que, según a la tienda virtual a la que acceden, deben informarse sobre los sistemas de cobro que aceptan o su nivel de seguridad.

Original recibido el 27-10-99

Aceptación definitiva: 12-12-99

En el proceso de comercio electrónico participan tres agentes principales: las empresas que actúan como proveedoras y como consumidoras, los usuarios que lo hacen como consumidores y las administraciones públicas que regulan las actividades que intervienen en la transacción, tanto si ésta se produce entre particulares como si es una relación entre el ciudadano y la administración (por ejemplo, el pago de impuestos).

Las estimaciones de la *Ocde* sobre volumen global del comercio electrónico superan los 300 millardos para los años 2001-2002 y el billón de US\$ hacia el 2003-2005. Sin embargo, las empresas que ya lo utilizan coinciden en que no se va a producir un crecimiento explosivo de esta actividad sino un desarrollo rápido y gradual.

La seguridad —tanto la física en el aspecto técnico como la psicológica desde la percepción del consumidor— es la clave que puede proporcionar la confianza necesaria que lance definitivamente el mercado del comercio electrónico. Este asunto es equiparable al dicho: “hecha la ley, hecha la trampa” es decir, lo que hoy es seguro en la Red, mañana puede dejar de serlo.

Internet tiene fama de insegura y el consumidor tiene miedo de que al proporcionar su número de tarjeta de crédito éste vaya a ser interceptado y utilizado de forma fraudulenta. A continuación se analizará este tema desde el punto de vista técnico y legal.

Aspectos jurídicos y de reglamentación

La generación de confianza en el comercio electrónico deberá pasar por la protección de la propiedad intelectual y de los datos personales, la promoción de una fiscalidad transparente —de forma que

no vaya a sufrir cargas mayores que las que soporta el comercio tradicional— y, naturalmente, por la creación de un marco de actuación interoperativo a escala mundial. Otros problemas a solucionar son la validez legal de las firmas digitales y de las autoridades de certificación.

1. ¿Qué es una firma digital?

El *Real Decreto-Ley 14/1999* de 17 de septiembre sobre firma electrónica, distingue y define:

a. Firma electrónica como el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o los autores del documento que la recoge.

b. Firma electrónica avanzada como la firma electrónica que permite la identificación del signatario y que ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

Según este *Decreto-Ley*, y de la misma forma que se ha recogido en las distintas directivas europeas sobre firma digital, ésta tiene el mismo valor jurídico que la convencional y será admisible en un juicio siempre que esté basada en un certificado conocido y que haya sido producida por un dispositivo seguro para su creación.

2. ¿Qué es un proveedor de servicios de certificación?

Los proveedores de servicios o autoridades de certificación, son aquellas personas físicas o jurídicas que

Para profundizar más en el tema

- *A common framework for electronic signatures*. Propuesta de directiva del Parlamento y el Consejo Europeos. COM (98) 297 final, 1998, mayo.
- *Common markup for micropayment per-fee-links*. W3C Working draft, 1999, agosto.
<http://www.w3.org/TR/WD-Micropayment-Markup/>
- *Información electrónica. España. 1997-2003*. Editor **Tomàs Baiget**. Institut d'Estadística de Catalunya. Asedie, 1999, junio.
<http://www.asedie.es/msstudy/>
- **Manasse, Mark S.** “The milliCent protocols for electronic commerce”.
<http://www.millicent.digital.com/works/detail/papers/>
- Payment mechanisms designed for the internet.
<http://ganges.cs.tcd.ie/mepeirce/Project/oninternet.html>
- **Rivest, Ronald L.** “Electronic lottery tickets as micropayments”.
<http://theory.lcs.mit.edu/~rivest/lottery.ps>
- **Rivest, Ronald L.; Shamir, Adi.** “PayWord and micromint: two simple micropayment schemes”, 1996, mayo, 7.
<http://theory.lcs.mit.edu/~rivest/publications.html>

responden de la exactitud de la información del certificado, que es lo que vincula los datos de verificación de firma a un signatario y confirma su identidad. Las autoridades de certificación aseguran el cumplimiento de los requisitos de su contenido mínimo:

- identificación de dicha autoridad,
- nombre y apellidos del titular del certificado o un seudónimo que conste de manera inequívoca,
- clave pública del titular,
- período de validez del certificado,
- código identificativo único del certificado,
- sus limitaciones de uso,
- límites de responsabilidad de la autoridad certificadora,
- valor de las transacciones,
- firma digital de la autoridad, y
- datos de creación de firma que se encuentran bajo el control del signatario.

Según el *Decreto-Ley* de la *Jefatura del Estado* mencionado anteriormente, y también según las directivas de la UE emitidas al respecto, los proveedores prestarán los servicios de certificación sin autorización previa y sin restricciones entre países miembros y cada nación debe garantizar que cumplan los requisitos suficientes exigidos por la legislación.

Para regular estas garantías, el *Consejo de Mercado Interior* aprobó en Bruselas el día 7 de diciembre de 1999 una directiva que crea el marco legal por el que se regula el comercio electrónico en la UE. Se pretende acercar las distintas posturas nacionales para alcanzar un régimen que garantice la libre circulación de servicios, las responsabilidades, los contratos, los códigos de conducta, la solución de litigios, los recursos judiciales y la cooperación entre estados miembros.

En España la *Secretaría general de comunicaciones* está trabajando en un proyecto de ley de comercio electrónico que se basará en el acuerdo político adoptado por el *Consejo de Ministros* de la UE.

Aspectos técnicos

Una transacción segura a través de internet debe:— Garantizar la confidencialidad, gracias al cifrado, de manera que los datos contenidos en las operaciones sólo sean accesibles para las partes que intervienen, evitando que un tercero pueda acceder a esa información.

— Mediante la utilización de las firmas digitales, asegurar la integridad de las transacciones, de tal for-

Recursos electrónicos especializados en el tema

1. Generales.

- ACE
<http://www.ace.es>
- @ece (Asociación española de comercio electrónico)
<http://www.aece.org/>
- CommerceNet
<http://www.commercenet.org>
- Lukasnet
<http://lukasnet.com>
- Virtu@l Cash
<http://www.banesto.es/banesto/virtual/castella/>

2. Sobre sistemas de pago en internet

- Cafe
<http://www.digicash.com/products/projects/cafe.html>
- CheckFree
<http://www.checkfree.com>
- CyberCash
<http://www.cybercash.com>
- DigiCash
<http://www.digicash.com>
- Financial services technology consortium
<http://www.fstc.org>
- Millicent
<http://www.research.digital.com/SRC/millicent/>
- Mondex
<http://www.mondex.com>
- NetBill
<http://www.ini.cmu.edu/NETBILL/>
- NetCash y NetCheque
<http://nii-server.isi.edu/info/netcash/>

ma que la información enviada no pueda ser alterada por terceros ajenos sin que lo advierta el destinatario.

— Proteger mediante el uso de la firma digital y la certificación, la autenticidad tanto del titular del medio de pago, como del proveedor. La firma digital garantiza la integridad de la transacción. La certificación por parte de un tercero garantiza la identidad de las partes que intervienen en el proceso.

— Garantizar la irrefutabilidad, que permite a cada lado de la comunicación probar fehacientemente que el otro lado ha participado en ella.

Los sistemas de seguridad se pueden dividir en dos grupos:

1. Canales seguros de comunicación. Agrupan un conjunto de protocolos que avalan la confidenciali-

dad y la integridad de las comunicaciones vía red. Destacan:

a. *Shttp (secure hiperText transfer protocol)* que proporciona las soluciones de seguridad a las conexiones http.

b. El protocolo *SSL (secure socket layer)* diseñado e implementado por *Netscape* que facilita sesiones de comunicación encriptadas y autenticación del servidor de forma que garantice la confidencialidad y autenticidad entre consumidor y vendedor.

c. El protocolo de *Microsoft (PCT)*, semejante al anterior pero compatible con otros.

2. Sistema de claves. Las técnicas criptográficas permiten que el usuario pueda ejecutar una clave desde cualquier lugar de la Red para así obtener seguridad en la transacción. Existen dos clases: cifrado simétrico y asimétrico.

a. Encriptación simétrica. Utiliza la misma clave para cifrar y descifrar —por ejemplo el sistema *DES (data encryption standard)* desarrollado por *IBM*—. Compartiendo los dos interlocutores una misma clave secreta y de longitud o complejidad suficientemente grande, permite garantizar la confidencialidad de la transacción entre ellos. Este sistema no es adecuado para comunicaciones esporádicas con muchas partes distintas, como suele ocurrir en el comercio electrónico, ya que antes de establecer cada una habría que intercambiar la clave secreta que se va a utilizar y hacerlo con algún procedimiento seguro.

b. Asimétrica o de claves públicas. Utiliza parejas de claves de tal manera que cada una de las claves puede cifrar información que sólo la otra puede descifrar. Cada par se asocia a una persona que da a conocer una (clave pública) para que se conozca ampliamente y mantiene en secreto la otra (clave privada) que solamente es conocida por su propietario. Esta última la guarda en su ordenador o en una tarjeta inteligente de tal forma que, para enviar un mensaje confidencialmente, basta con cifrarlo con la pública del destinatario para que éste pueda descifrarlo con la suya privada que sólo él conoce, así no es necesario intercambiar previamente ninguna clave. Para evitar suplantaciones sería necesario contar con una autoridad de certificación que acredite las públicas de cada persona o entidad. En esto se basa el sistema *RSA* (acrónimo formado por las iniciales de sus creadores **R**ivest, **S**hamir y **A**delman).

Los sistemas de clave asimétrica permiten garantizar la integridad, autenticidad e irrefutabilidad que veíamos antes por medio de las firmas digitales. Se extrae un “resumen” (o *hash*) del mensaje, se cifra con la clave privada del remitente y se añade al final del men-

saje. Se envía todo esto cifrado con la clave pública del destinatario. Cuando éste recibe el mensaje, lo descifra con su clave privada y comprueba la firma, sabiendo la clave pública del remitente. Si el mensaje puede descifrarse con la clave pública, significa que sólo pudo ser cifrado con la privada del remitente y que no ha sido alterado en su paso por la Red. El receptor está así seguro del origen de la nota (autenticidad), y quién la ha enviado no podrá negar haberlo hecho (irrefutabilidad). La estructura que mueve este modelo, incluyendo a las autoridades de certificación, se llama *infraestructura de clave pública (PKI: public key infrastructure)*. Su principal inconveniente es la lentitud en el proceso y la necesidad de la intervención de terceros, es decir, las autoridades de certificación.

c. El protocolo *SET*. Ha sido desarrollado por *MasterCard* y *Visa*, con la colaboración de *IBM*, *Microsoft* y *Netscape*, e incorpora los dos sistemas de cifrado simétrico y asimétrico con el fin de realizar operaciones con tarjeta de crédito a través de internet, tanto en tiempo real (a través de web) como en diferido (a través del correo electrónico). Aprovecha la rapidez de los primeros pero además utiliza las autoridades de certificación y las firmas digitales. Es un protocolo abierto para que cada uno desarrolle las implementaciones en distinto software. En este momento la dificultad y el costo de su utilización lo hace entrar en competencia directa con el protocolo *SSL*, calculándose que para el año 2003 el 90% de todas las transacciones del mundo se llevarán a cabo a través de éste y menos del 10% utilizará *SET*.

La diferencia entre ambos es que *SSL* proporciona encriptación de canales pero no valida ninguna de las partes que ejecutan la operación, lo que deja dudas acerca de quiénes son y en cierta forma protege menos contra el fraude. *SET*, sin embargo, verifica la autenticidad de los involucrados, pero es un sistema complicado y costoso de implementar. En España, la *Agencia de certificación electrónica* emite ya estos certificados, aunque su establecimiento está siendo lento.

Sistemas de pago

Actualmente existen múltiples y variados modelos de pago en internet: unos ya establecidos, otros en pruebas, algunos son simples propuestas, unos que se basan en reproducir de forma virtual los métodos del comercio tradicional —como los cheques o las tarjetas de crédito— y otros que establecen nuevos procedimientos como el dinero electrónico.

Martín Becerra Olmos² los clasifica en cuatro categorías a tenor de su integración con los sistemas financieros de pago:

— Comunicación protegida: se ampara el intercambio de datos pero el proceso de pago se realiza fuera de internet. No existe ninguna integración electrónica con los sistemas de pago. El comprador informa al vendedor a través de la Red de los datos de su tarjeta de crédito —del mismo modo que lo hubiera hecho a través del teléfono— enviándolos y recibiendo los encriptados a través de los protocolos soportados por los navegadores como *SSL* o *Shhttp*.

— Intermediarios con el sistema financiero: trabajan con cuentas individuales que son periódicamente liquidadas contra tarjetas de crédito o cuentas bancarias, por lo que todas las operaciones acumuladas comparten los gastos de una misma transacción, lo que reduce los costos del proceso y lo valida para operaciones de bajo importe.

— Integrados en el sistema financiero: combinan un intercambio seguro de datos de pago con procedimientos de autorización automatizados mediante conexión individual en tiempo real con los sistemas financieros.

«Las estimaciones de la Ode sobre volumen global del comercio electrónico superan el billón de US\$ hacia el 2003-2005»

— Dinero electrónico: se basa en la creación de unas unidades monetarias que funcionan como si fueran efectivo y que están representadas por una serie de informaciones que les permiten circular con valor en sí mismas. El dinero se almacena en un monedero o *wallet* del ordenador. Éste es el verdadero sistema orientado a la realización de micropagos, diseñado para que exista un absoluto anonimato, de manera que preserve la privacidad del poseedor.

Los medios de pago que existen en el mundo “real” (no digital) son fruto de una larga evolución, y cada uno de estos sistemas —efectivo, cheque, tarjetas de crédito, etc.— ha nacido para satisfacer determinados requerimientos, en ocasiones sustitutos entre sí, aunque en realidad complementarios. Para pequeñas cantidades se utiliza el efectivo, fácil de transportar y completamente anónimo, sin intervención de terceros. En el caso de importes medianos y ocasionales (es decir, de carácter no repetitivo) se utilizan las tarjetas de crédito, proceso en el que ya no sólo se implican comprador y vendedor sino también otros agentes como los bancos y las redes de operaciones de tarjeta. Para pagos que van de sumas medias a grandes se utilizan cheques y órdenes de pago para los que se realizan con carácter repetitivo, como las domiciliaciones en cuen-

ta. En ellos también intervienen terceros como los bancos o entidades financieras. Este mismo esquema se representa en la Red.

Pago con tarjeta de crédito a través de internet

Hasta ahora el sistema más generalizado en la Red ha sido la tarjeta de crédito. Cuando se realiza una transacción electrónica con este método, el modelo que se reproduce es el mismo que al realizar una compra en un comercio tradicional. Tan sólo se diferencia en el transporte —que se realiza a través de la Red en lugar de teléfono— y en el grado de confianza. Las tarjetas de crédito no sólo son ya un sistema de pago probado y utilizado en el comercio tradicional sino que, además, gozan de aceptación internacional. Sin embargo presenta algunos inconvenientes: en cuanto a la seguridad —ya que hay que proporcionar al vendedor el número de la tarjeta—, en lo referente al costo de la transacción —el emisor de la tarjeta carga gastos de transacción al vendedor— y la necesidad de poseer una tarjeta de crédito en activo. En este campo destaca el protocolo *SET* comentado anteriormente.

Un ejemplo fue *FVH* (*First virtual holdings*) una de las primeras empresas en idear un modelo de pago para internet que funcionaba mediante dos sistemas integrados: mensajes de correo electrónico (de seguridad relativa) y las redes habituales de tarjetas de crédito (más seguras). El usuario abría una cuenta en *FVH* y periódicamente liquidaba los cargos contra una tarjeta de crédito. Solicitaba un número de identificación personal (*PIN*) y una sola vez —por correo postal, electrónico o por fax— proporcionaba los datos de su tarjeta. Cuando hacía una compra lo que facilitaba era el *PIN*, el comercio solicitaba confirmación a *FVH* y ésta, a su vez, autorizaba al cliente por medio del correo electrónico.

La seguridad de no sufrir un uso fraudulento —por interceptación del *PIN*— junto con una cuenta de correo del cliente más bien deficiente, a lo que había que sumar la inseguridad del cobro por parte de los comerciantes si en última instancia el comprador negaba la autorización, son algunos de los problemas de su utilización. Ahora *FVH* recomienda a sus antiguos clientes que se sumen al sistema *CyberCash* que protege la presentación de la tarjeta de crédito, establece una pasarela entre internet y las redes de autorización y, además, procesa las transacciones individualmente y en tiempo real, obteniendo así las autorizaciones en unos 20 segundos.

Este sistema trabaja con el concepto de monedero electrónico o *wallet*, residente en el ordenador del usuario, al que se accede mediante clave y en el que

están registrados todos los números de tarjetas de crédito del consumidor. En un proceso inicial único, éste contacta con *CyberCash* para la descarga del software que creará su monedero y se generan un par de claves de tipo pública/privada, enviando la primera a *CyberCash*. Desde el monedero indica qué tarjeta utilizará, información que pasa encriptada al comercio, el cual, a su vez la envía a *CyberCash* junto con su propia versión de la operación. En este momento se descifran ambas informaciones y se comparan para verificar que son coincidentes. Si no hay problema la autorización recorre el camino inverso hasta llegar al cliente.

Cheques y órdenes de pago electrónicas

Entre empresas es más frecuente el pago mediante cheques que el uso de la tarjeta de crédito. Los cheques electrónicos reducen el coste de proceso y aumentan la seguridad, mediante la utilización de la firma digital. Se crea el equivalente a uno común que puede ser transmitido electrónicamente y que tiene como consecuencia la transferencia de fondos desde una cuenta bancaria dentro de la estructura tradicional.

Más información sobre el comercio electrónico:

ACE
<http://www.ace.es>

@ECE
<http://www.acece.org/>

CommerceNet
<http://www.commercenet.org>

Lukasnet
<http://www.lukasnet.com>

Virtu@l Cash
<http://www.banesto.es/banesto/virtual/castella>

Ejemplo de este sistema es *eCheck* —definido por el *Fstc* (*Financial service technology consortium*)— que asume la disponibilidad amplia de claves públicas y de tarjetas inteligentes para almacenarlas de forma segura. El consumidor envía a través de internet un cheque firmado electrónicamente al comercio; éste lo pasa a su banco, también mediante internet, endosado con su firma electrónica. Si el cheque es de un tercer banco, el del comerciante lo envía electrónicamente a compensar a través de las redes tradicionales. Otro ejemplo de este sistema es *NetCheque* que, básicamente, reproduce en la Red el sistema usual de emi-



sión y compensación de cheques.

Dinero electrónico

Todos los sistemas que se han visto anteriormente sirven para realizar transacciones electrónicas sobre dinero convencional. El dinero electrónico se puede definir como la creación de unas unidades monetarias —como si fueran efectivo que tiene forma digital, secuencias de bytes que se transmiten a través de la Red— que representan un valor en sí mismas y que se almacenan en monederos electrónicos o simplemente como ficheros en el ordenador. Se basan en el prepa- go, es decir, convierten previamente dinero real en electrónico. Para certificar su valor el banco emisor utiliza su firma digital, se lo entrega al consumidor que lo ha pedido y carga en la cuenta de éste la misma cantidad en dinero real. Una vez creados pueden conservarse, utilizarse para realizar una compra o un pago o volver a convertirse en dinero convencional.

Se caracterizan por el bajo coste de las transacciones —por lo que son los más indicados para efectuar micropagos—, su rapidez, su funcionamiento sin autorización previa y que son anónimos. Estas características los convierte en potenciales conflictos desde el punto de vista gubernamental ya que escapan a las políticas monetarias sobre creación de dinero y porque, al emular el efectivo, se prestan a ser utilizadas para el blanqueo de dinero.

Micropago

Hasta ahora, como ya se ha comentado anteriormente, el procedimiento de pago más utilizado es mediante la encriptación de los datos de una tarjeta de crédito. Sin embargo hay servicios en internet cuyo coste, al ser tan bajo, no hace rentable un modelo cuya media ideal de transacción son los 60 US\$. Si a un vendedor le paga con un cheque una venta de 1.000 PTA, el banco le cobra un mínimo de cien por negociarlo, lo que supone un coste directo del 10% sobre las ventas. Algunos productos digitales son de bajo importe, como una canción o un artículo de una revista, que pueden tener un precio, por ejemplo en el caso de una fotocopia, de 100 PTA. Se podría definir, por tanto, micropagos como las transacciones financieras electrónicas de escaso valor, que pueden ir desde 1 a 1.000 PTA.

El coste de las operaciones determina la viabilidad de algunos servicios, especialmente los de bajo precio, es decir los micropagos. Los gastos de procesar un pago están formados por los recursos que consumen las actividades que hay que realizar y por las comisiones de los sistemas externos. Para reducir esta inversión en

recursos se tiene que descender el nivel de las actividades manuales y tratar de que todo el proceso se lleve a cabo de forma electrónica, para lo que sería preciso interoperabilidad y normalización entre los modelos de pago existentes.

Las propiedades deseables que deberían poseer, económicamente hablando, serían: transacción a bajo coste, una base grande de clientes —lo que se conoce como “masa crítica”— e interoperatividad entre sistemas tecnológicos diferentes.

Desde el punto de vista de la sociedad estas características serían:

— Anonimato: ya que cuando un usuario paga un servicio con monedas reales nadie puede conocer su identidad, mientras que el pago mediante tarjeta de crédito no respeta esa máxima. A medida que el dinero electrónico ha ido apareciendo la intromisión en la privacidad se ha facilitado mucho más.

— Divisibilidad: la unidad de moneda electrónica debe ser fácilmente fraccionable de forma que permita efectuar micropagos por cantidades casi insignificantes. Algunos sistemas como *Millicent* se han diseñado sólo para pequeños gastos y otras como *Cybercash* contemplan pagos mayores o micropagos con dos sistemas distintos.

— Seguridad: que evite el uso fraudulento y la falsificación así como garantía en el cobro para los comerciantes e intermediarios.

A corto plazo el dinero digital es sólo una forma más conveniente del ya existente, pues se crea a partir de él. Pero a largo plazo podría crearse por cuenta propia si los usuarios aceptan su valor fiduciario; al fin y al cabo un billete es sólo un trozo de papel de colores.

Algunos de los sistemas de micropago son:

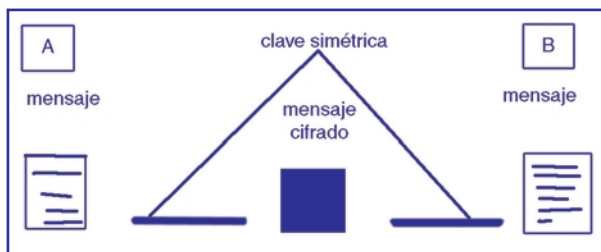
— *Cybercoin*: es el procedimiento de *CyberCash* incluido en la versión para *Windows* de su monedero electrónico, muy apropiado para realizar pagos pequeños (a partir de 35 PTA). Requiere cargar previamente este monedero a partir de una cuenta o tarjeta de crédito. Sus propios ordenadores controlan las cuentas de sus clientes limitando cada una a 1.500

PTA. Cuando un usuario realiza un gasto de unas 50 PTA, por ejemplo, todo se realiza bajo el dominio de *CyberCash* sin necesidad de utilizar el sistema financiero tradicional. Al pagar, el consumidor proporciona un número de cuenta y la autorización para que le carguen el gasto, y el vendedor lo remite al servidor central de *CyberCoin* donde se deduce el gasto de la cuenta del usuario.

<http://www.cybercash.com>

— *DigiCash*, a través de su producto *E-Cash*, es el pionero del dinero electrónico. Para utilizarlo, el primer requisito es abrir una cuenta en un banco real —en cualquiera de los que trabajan con él—. La propia institución bancaria suministra un cd-rom con el software del monedero electrónico, en versiones para *Windows* y *Unix* y adaptable a *OS/2*. Además proporciona un identificador y una contraseña que hay que utilizar al iniciar la instalación pero que nunca serán accesibles al vendedor. Cuando realice una compra su importe se descontará de su monedero y el usuario podrá, en todo momento, comprobar los apuntes de la cuenta y el estado de sus fondos. El sistema es absolutamente centralizado sin la actuación de intermediarios.

<http://www.ecashtechologies.com>



Más información sobre distintos sistemas de pago en internet

Cafe	http://www.digicash.com/products/projects/cafe.html
Checkfree	http://www.checkfree.com
Cybercash	http://www.cybercash.com
Digicash	http://www.digicash.com
Financial Services Technology Consortium	http://www.fstc.org
Millicent	http://www.research.digital.com/SRC/millicent/
Mondex	http://www.mondex.com
Netbill	http://www.ini.cmu.edu/NETBILL/
NetCash and NetCheque	http://nii-server.isi.edu/info/netcash/

— *Millicent* ha llegado a concebir una auténtica estructura monetaria virtual. Su sistema de funcionamiento es: un usuario adquiere en un intermediario (*broker*) elegido por él un número determinado de unidades de pago (que ellos llaman *scrip*) que se incorporan a su monedero electrónico del tal forma que, al hacer una compra en internet, el valor de lo adquirido se descarga automáticamente de su monedero, incluso para micropagos del montante de 1 PTA. El intermediario se encarga de proporcionar los *scrip* al consumidor y descontar su valor real de la cuenta bancaria o tarjeta de crédito proporcionada por él para, posteriormente, convertir de nuevo en dinero convencional aquellos que le presentan los vendedores adscritos al sistema.

<http://www.millicent.com>

La descarga del software y la instalación del monedero es gratuita y muy sencilla, disponible en versión *Windows95/NT*. Puede hacerse directamente desde la página web o solicitar que la proporcionen en un cd-rom. El sistema permite al usuario pagar cantidades muy pequeñas con la frecuencia que necesite. Respeta el anonimato ya que el intermediario conoce la identidad del usuario pero no sabe para qué utiliza los *scrip* que compra, mientras que el vendedor conoce el objeto que vende pero no la identidad del consumidor. La desventaja es que tiene que comprar en lugares adscritos al modelo.

— *NetBill* es, sin duda, el sistema preferido para comprar productos digitales como programas de ordenador y aplicable perfectamente a las operaciones del préstamo interbibliotecario, al acceso a una base de datos o al procedimiento de “pagar por ver” un artículo en una revista electrónica.

<http://www.netbill.com>

Utiliza una mezcla de claves simétricas y parejas de claves criptográficas o asimétricas y requiere que el usuario haya abierto previamente una cuenta en el servidor *NetBill*. El proceso se realiza de la siguiente manera: el comerciante envía el objeto de compra en formato encriptado al ordenador del usuario, el software instalado por *NetBill* en él comprueba que la compra ha llegado intacta y notifica esto al vendedor, el cual envía este mensaje de verificación del usuario junto con los datos de su cuenta y la clave de descryptación al servidor *NetBill*, que confirma que en la citada cuenta hay fondos suficientes para pagar la compra. Si es así, los transfiere, almacena la clave y rinde cuentas de todas estas acciones al vendedor. Éste a su vez envía al comprador la clave que descrypta la compra. Si antes de completar este último paso se produjera algún fallo, el comprador podría retirar esta clave directamente en el servidor de *NetBill*.

— *Café* (*conditional access for europe*) es el monedero electrónico desarrollado bajo el proyecto europeo *Esprit* (*European strategic programme for research in information technology*), y está diseñado originalmente para compras en comercios, más que para su utilización a través de la Red, utilizando las *smart-cards* o tarjetas inteligentes como mecanismo de almacenaje de dinero digital. La filosofía es permitir un sistema de pago pan-europeo que soporte diferentes monedas. Mantiene un registro de todas las cantidades gastadas para evitar el fraude de abonar dos veces el mismo dinero. La moneda que utiliza está encriptada, todos los pagos van acompañados de una firma digital y además la identidad del usuario aparece codificada en el número de cada moneda. Las transacciones se realizan en un doble modelo offline y online.

Como iniciativas españolas cabría destacar *Virtual Cash* —la tarjeta gratuita de *Banesto*— sin chip ni banda magnética, que el usuario debe solicitar mediante formulario previa apertura de cuenta y que asigna un número de identificación personal para comprar en internet e *Infovía* en los comercios adheridos al sistema tecleando los datos identificativos de la tarjeta. El comerciante no conoce en ningún momento los datos personales de su cliente. Aunque *Banesto* fue probablemente el primer banco en poner en marcha este servicio, otras entidades españolas lo ofrecen ya y muchas otras lo harán en el futuro.

<http://www.banesto.es/>

Micropago y bibliotecas o centros de documentación

Muchos de los servicios que estos centros ofrecen o reciben están basados en el pago de pequeñas cantidades que se giran periódicamente a cuentas concertadas por los usuarios correspondientes. Como se ha visto a lo largo de este artículo, estos sistemas de pago que se desarrollan en el sistema financiero tradicional podrían adaptarse perfectamente en el sistema de pago digital.

Cuando realizan una fuerte inversión —por ejemplo en la adquisición de un lote de libros o una suscripción completa a una revista— o para la compra de material fungible o de mobiliario, podría utilizar como sistemas de pago cheques electrónicos o tarjetas de crédito como los ya comentados anteriormente en los distintos apartados, es decir, un sistema como *CyberCash*, *E-Check* o *DigiCash*.

Sin embargo, para los servicios que el propio centro proporciona, el procedimiento de pago debería ser diferente ya que raramente tienen importes elevados. Serían aquí muy útiles los ejemplos de *CyberCoin*, *Millicent* y, al ser en muchos casos productos digitales los

que se suministran, especialmente provechoso sería el sistema *NetBill*.

Un ejemplo podría ser el préstamo interbibliotecario que todas las bibliotecas poseen. Aunque en muchas se continúan utilizando las fotocopias, en otras ya se envían los artículos escaneados a una cuenta de correo electrónico o un servidor determinado. Un muestra de este sistema de funcionamiento es *Ariel*.

<http://www.doc6.es>.

De la misma forma que se hace un cargo —que puede ir desde una a varias páginas fotocopiadas— a la cuenta proporcionada por el usuario, éste podría estar adherido a uno de los sistemas digitales antes mencionados, lo que mejoraría la seguridad, la comodidad y permitiría realizarlo cada vez que fuera necesario y no tener que esperar a acumular varios para que la operación sea rentable.

Otro ejemplo de estos micropagos, a los que los centros de información se enfrentan, sería el suministro de sentencias o búsquedas en bases de datos, por los que se cobra una cantidad por la consulta y otra por los resultados obtenidos, que nunca suelen ser muy grandes.

Del mismo modo, el adoptar un procedimiento de pago electrónico afectaría a los servicios de bajo precio que las bibliotecas contratan con proveedores de información, como el importe que se abona por registro recuperado o tiempo de conexión a una base de datos determinada, o el pagar por ver un artículo de una publicación en concreto.

Si los sistemas de micropago acaban por adoptarse en las bibliotecas y centros de documentación con servicios de valor añadido, esto redundará en beneficio tanto de los usuarios como de los propios centros, que se convertirán intermediarios entre el usuario y los proveedores de información y se simplificaría la complicada tarea que los servicios de gestión de cada biblioteca realizan en este momento en cuanto a identificación y cargo a los distintos consumidores.

Dos ejemplos de proyectos europeos de empleo de *smartcards*, en el ámbito bibliotecario son la aplicación de *Mondex* en la *Universidad de Exeter* o el proyecto *Tolimac* que se ha desarrollado en la *Université Libre de Bruxelles* dentro del *Cuarto programa marco de investigación y desarrollo tecnológico*, bajo el *Programa de aplicaciones telemáticas-Sector bibliotecas (DGXIII-E4)*. Las *smartcards* tienen una baja capacidad de almacenamiento, sin embargo las *lasecards*, que son soportes mucho más potentes, permitirían, no sólo realizar pagos digitales sino que, además, son capaces de guardar toda la información que identifica al

usuario: su perfil en préstamos o búsquedas, su expediente académico, etc.

<http://www.mondex.com>

<http://tolimac.ulb.ac.be/>

<http://www.ex.ac.uk>

Notas

1. *Estudio de situación del comercio electrónico en España*. Ministerio de Fomento, Secretaría general de telecomunicaciones, 1999, mayo. <http://www.sgc.mfom.es/sat/ce/indice.html>

2. **Becerra Olmos, Martín**. "6 modelos de pago en internet". En: *Estrategia financiera*, 1997, junio, n. 130.

Bibliografía

Balzano, Marta. "Comercio electrónico (medios de pago)". En: *LukasNet Communication*. <http://lukasnet.com/pymel/ir/250599.htm>

Becerra Olmos, Martín. "6 modelos de pago en internet". En: *Estrategia financiera*, 1997, junio, n. 130.

Camp, L. Jean; Sirbu, Marvin; Tygar, J. D. "Token and notational money in electronic commerce". <http://www.ini.cmu.edu/netbill/pubs/camp/usenix.html>.

Estudio de situación del comercio electrónico en España. Ministerio de Fomento, Secretaría general de telecomunicaciones, 1999, mayo. <http://www.sgc.mfom.es/sat/ce/indice.html>

Estudio sobre comercio electrónico entre empresa y consumidor, en Internet y en España: avance de las principales conclusiones. Asociación española de comercio electrónico @ECE, 1998, noviembre. <http://www.aece.org/infodocumento/estudio.htm>

FAQ: Usos business-to-market. <http://www.commercenet.org/faq/ec4.htm>

Gómez, José Manuel. "Dinero digital". En: *iWorld*, año II, 1998, octubre, n. 9. <http://www.idg.es/iworld/199810/articulos/dd.asp>

Herrero Solana, Víctor. "Aplicación de smartcards y lasecards en el ámbito bibliotecario". En: *El profesional de la información*, 1998, octubre, v. 7, n. 10, pp. 12-18.

"La info y el comercio electrónico". En: *LukasNet communication*. <http://lukasnet.com/pymel/iq/290499.htm>

NetBill: an internet commerce system optimized for netWork delivered services. <http://www.ini.cmu.edu/netbill/pubs/CompCon.html>

Real Decreto-Ley 14/1999 de 17 de septiembre sobre firma electrónica. En: *BOE*, 1999, 18 de septiembre, n. 224.

Ribas, Xavier. "Emisión de dinero electrónico". En: *Contract-soft*. <http://www.onnet.es/08008007.htm>

Ribas, Xavier. "Sistemas de pago electrónico del euro en tiempo real". En: *Contract-soft*. <http://www.onnet.es/08008008.htm>

Schöter, Andreas; Willner, Rachel. "Digital money online: a review of some existing technologies". En: *Intertrader Ltd.*, 1997, febrero. <http://www.intertrader.com/library/DigitalMoneyOnline/dmo/dmo.htm>

Cristina García Testal. *Biblioteca de ciencias sociales Grogori Maïans*. Universidad de Valencia. Cristina.Garcia-testal@uv.es